IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

DAVID MACNEIL, 84 Isla Bahia Dr. Fort Lauderdale, FL 33316 *Plaintiff,* v. BOOZ ALLEN HAMILTON, INC, 8283 Greensboro Dr McLean, VA 22102 **SERVE ON:** Registered Agent The Corporation Trust, Inc. 2405 York Road Suite 201 Lutherville Timonium, MD 21093 *Defendant.*	Case No.:

COMPLAINT

Plaintiff, David MacNeil ("Plaintiff" or "MacNeil"), brings this Complaint against Defendant, Booz Allen Hamilton, Inc. ("Defendant" or "Booz Allen"), and alleges as follows:

1. This suit arises from Booz Allen's systemic failure to safeguard its computer systems, failure to protect IRS networks and databases, and failure to monitor and restrict its personnel's data access, at the expense of the confidential tax return information of thousands of American taxpayers—including Plaintiff.

2. Since at least 2008, Booz Allen has operated under one or more multimillion-dollar contracts with the Department of the Treasury or the IRS, through which Booz Allen accessed and reviewed tax returns and return information in the course of performing IT, data processing,

cybersecurity, and tax administration services for the IRS. Despite its knowledge of criminal consequences for unauthorized inspection or disclosure, and federal obligations to safeguard this data, Booz Allen chose not to protect these confidential tax returns and return information.

3. Instead, Booz Allen willingly allowed its employees unrestricted and unmonitored access to IRS databases and systems. This access enabled Booz Allen employees to run tailored searches to retrieve personally identifiable taxpayer data, including returns and return information, dating over a fifteen-year period. Booz Allen enabled its employees to search IRS databases using specific keywords, as well as more generalized search parameters. Booz Allen further permitted private downloads of the confidential information to local machines and private uploads of the taxpayer data to remote and cloud-based storage—all without sufficient tracing, monitoring, or security in place. In effect, Booz Allen permitted its employees free rein with confidential taxpayer data, in derogation of its duty to American taxpayers, including Plaintiff Mr. MacNeil.

4. This laxity soon delivered disastrous, but predictable, consequences. Beginning in 2018, Booz Allen's systemic failures converged in a massive data theft perpetrated by its employee Charles "Chaz" Edward Littlejohn ("Littlejohn").

5. Littlejohn is a person who was employed by Booz Allen at various intervals from 2008 to 2021. Littlejohn performed work under Booz Allen's contracts with the Department of the Treasury and/or the IRS. At all relevant times, Booz Allen afforded Littlejohn access to IRS systems and databases that contained the confidential tax returns and tax return information of thousands of American taxpayers, including Plaintiff.

6. During his Booz Allen tenure from 2018 to 2021, Littlejohn used his Booz Allen credentials to search for and download the tax returns and return information of thousands of the nation's wealthiest taxpayers, including President Donald Trump, Jeff Bezos, Elon Musk, Warren

Buffet, and Michael Bloomberg. The stolen information also included the tax returns and return information of Plaintiff.

7. On multiple occasions, Charles Littlejohn uploaded this stolen tax information to a private website. He then disclosed portions of the data to ProPublica and other media outlets, including The New York Times. ProPublica has since published nearly 50 articles using the stolen tax data on these wealthy Americans. The articles included a high-profile piece by ProPublica that purportedly summarized how tax loopholes were allegedly utilized by Mr. MacNeil, titled "How the Trump Tax Law Created a Loophole That Lets Top Executives Net Millions by Slashing Their Own Salaries."[1] The leading page of the article appears below:

8. The article mischaracterized Mr. MacNeil's tax records and payments, falsely suggesting that he, as the owner of WeatherTech Direct, LLC, illegally took an unreasonably low salary for the purpose of avoiding taxes. The article said he "saved an estimated $8 million in the

[1] ProPublica, *How the Trump Tax Law Created a Loophole That Lets Top Executives Net Millions by Slashing Their Own Salaries*, PROPUBLICA (August 19, 2021) https://www.propublica.org/article/how-the-trump-tax-law-created-a-loophole-that-lets-top-executives-net-millions-by-slashing-their-own-salaries.

first two years, according to a ProPublica analysis of the IRS records." The piece proceeded to list further details from Mr. MacNeil's tax information, including specifics on his real and personal property.

9. ProPublica later issued a story entitled "Ken Griffin Spent $54 Million Fighting a Tax Increase for the Rich. Secret IRS Data Shows It Paid Off for Him."[2] The article used confidential tax returns and return information to malign Plaintiff and other taxpayers further: "Some of the state's richest people spent big to defeat a ballot initiative that would have enabled a higher tax rate on the rich. Using IRS data, ProPublica estimated how much some of the biggest backers saved when the measure failed." The article then included a comparison of Mr. MacNeil's alleged "estimated annual tax savings," "annual income" and "campaign donation records."

10. Booz Allen's theft and disclosure through Littlejohn was not limited to a few isolated returns. Indeed, ProPublica claims to have received not just tax returns, but also information that is sent to the IRS about financial activities such as "income and taxes," "investments, stock trades, gambling winnings and even the results of audits.[3]" In fact, even Congress confirmed there was "little doubt" that the leaked information to ProPublica—including Plaintiff's confidential tax information—"came from inside the IRS" database, and that the disclosure was "precisely what 26 U.S.C. § 6103 and related statutes were designed to prevent—the disclosure of private tax information and the political weaponization of that information."[4]

[2] ProPublica, *Ken Griffin Spent $54 Million Fighting a Tax Increase for the Rich. Secret IRS Data Shows It Paid Off for Him*, PROPUBLICA (July 7, 2022) https://www.propublica.org/article/ken-griffin-illinois-graduated-income-tax.

[3] ProPublica, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax*, PROPUBLICA, (June 8, 2021), https://www.propublica.org/article/the-secret-irs-files-trove-of-never-before-seen-records-reveal-how-the-wealthiest-avoid-income-tax.

[4] Letter from Congressman Kevin Brady and Senator Mike Crapo to The Honorable Janet Yellen, Secretary of the U.S. Department of Treasury (April 18, 2022), https://gop-waysandmeans.house.gov/wp-content/uploads/2022/04/4-18-2022-Brady-Crapo-to-Yellen_FINAL.pdf.

11. Littlejohn, Booz Allen's employee, ultimately pleaded guilty to a violation of 26 U.S.C. § 7213(a)(1) for unlawful disclosure of confidential tax return information. In that plea, he admitted that, while working for Booz Allen, he had access to unmasked IRS data associated with thousands of the nation's wealthiest people, and that he exploited that access to unlawfully inspect and repeatedly disclose confidential tax return information to media outlets.[5] Since that publication, and its highly misleading characterization of his tax return history, Mr. MacNeil has faced ongoing injury including, but not limited to, public backlash, significant reputational harm, and loss of privacy, and economic damages.

12. On October 5, 2023, Mr. MacNeil received a letter from the U.S. Department of Justice informing him that he was a victim or potential victim in the criminal case against Littlejohn. (Attached as "Exhibit **A**").

13. Accordingly, Plaintiff brings this action against Booz Allen for violations of federal law and invasion of privacy, including (a) its employee's unlawful inspections and disclosures of Plaintiff's confidential tax return information, (b) its willful and intentional failure to establish appropriate administrative, technical, and/or physical safeguards over access to IRS tax data by employees such as Littlejohn, and (c) its failure to ensure the security and confidentiality of Mr. MacNeil's confidential tax return information.

JURISDICTION AND VENUE

14. This Court has personal jurisdiction because the unlawful inspections, thefts, and disclosures of Plaintiff's tax returns occurred, in whole or in part, in Maryland and arose from Booz Allen's IRS contract work performed in Maryland, including by Littlejohn.

[5] *United States v. Charles Edward Littlejohn,* 1:23-cr-343 (D.D.C.) (ECF 9, ¶ 10–13, Oct. 12, 2023).

15. On information and belief, Littlejohn worked for the IRS and Booz Allen in Lanham, Maryland, at the IRS's New Carrollton Federal Building, which houses many of the IRS's IT functions.

16. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1331 because the first cause of action arises from federal statute. The Court has subject-matter jurisdiction over the remaining causes of action under 28 U.S.C. § 1367 because the claims are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy. Additionally, 26 U.S.C. § 7431(a) authorizes suit in a district court of the United States for the unauthorized disclosure or inspection of tax return or return information.

17. Venue lies in the District of Maryland pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred there.

PARTIES

18. Plaintiff David MacNeil is a self-made entrepreneur and the founder and owner of WeatherTech Direct, LLC, ("WeatherTech"), a company known for producing high-quality automotive accessories, including floor mats, cargo liners, and other protective products. Mr. MacNeil founded WeatherTech approximately thirty-five years ago out of his own home. WeatherTech is dedicated to investing in American manufacturing and the American economy, and 95% of its products are made in its own factories within the United States. Mr. MacNeil is a resident and citizen of the State of Florida.

19. Defendant Booz Allen Hamilton, Inc. is an American government and military contractor of over 32,000 employees, purportedly specializing in intelligence. Booz Allen is incorporated under Delaware law and headquartered in McLean, Virginia. The company provides

consulting, analysis, and engineering services to public and private-sector organizations and nonprofits, including the Department of the Treasury and Internal Revenue Service.

FACTUAL ALLEGATIONS

A. The IRS's Flawed Cybersecurity Infrastructure

20. The IRS relies heavily on IT systems and electronic data to collect, process, analyze, and maintain tax returns and return information. But while that reliance has increased, the IRS's cybersecurity protections remain woefully inadequate. The Treasury Inspector General for Tax Administration ("TIGTA") has repeatedly documented these system threats.

21. For example, a 2018 TIGTA audit identified 88 separate physical security control weaknesses and over 1,700 improperly configured user accounts within the IRS.[6] TIGTA also found that the IRS's Windows Policy Checker was out of date and used three-year-old technical guidelines to conduct its analysis.[7] As a result, TIGTA concluded "the IRS cannot ensure that sensitive taxpayer information and taxpayer dollars are preserved and protected.[8]

22. Despite annual audits, TIGTA continued to find systemic failures by the IRS to establish appropriate administrative, technical, and physical safeguards to adequately protect against the unlawful disclosure of taxpayers' confidential tax return information. For example, in its *Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2020*, TIGTA revealed that the IRS had failed to use "encryption algorithms" in accordance with Federal Information Processing Standards 140-2, *Security Requirements for Cryptographic Modules* for certain operating systems in order to keep confidential tax return information "unreadable for an

[6] *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, REPORT NO. 2018-20-034, ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT AND CRIMINAL INVESTIGATION COMPUTER ROOMS LACK MINIMUM SECURITY CONTROLS, at *Highlights* (June 27, 2018).
[7] *Id.*
[8] *Id.* at 5.

unauthorized user."[9] Likewise, TIGTA reported that 2 out of 5 of the IRS's Cybersecurity Framework Function Areas (i.e., Identify, Protect, Detect, Respond, Recover) "were deemed as 'not effective.'"[10]

23. TIGTA has also identified multiple security deficiencies for the IRS system that collects, converts, and stores a taxpayer's confidential tax return information into electronic records of taxpayer data. The deficiencies included "more than 16,000 policy violations."[11] In other instances, "the IRS inappropriately assigned business role accounts to an administrator group, resulting in those accounts [and thus inappropriate employees] having unnecessary elevated privileges."[12] Notably, TIGTA found that the IRS "lacked management oversight to ensure that Federal and [Internal Revenue Manual] requirements are met" and, in "critical areas" housing computer rooms, "the IRS cannot control the movement of individuals and eliminate unnecessary traffic throughout this critical security area [to] reduce the opportunity for unauthorized disclosure or theft of tax information." [13]

24. Not only did TIGTA, through its various audits, put the IRS on notice for years of the IRS's security deficiencies, but the IRS had first-hand knowledge of its vulnerabilities based on repeated data breaches. For instance, from 2014–2015, approximately 400,000 U.S. taxpayer accounts were potentially accessed by hackers, with hundreds of thousands of additional accounts targeted.[14] Then, in 2017, IRS data from approximately 100,000 taxpayers was potentially

[9] *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, REPORT NO. 2021-20-001, ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE'S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2020, at 22 (Oct. 30, 2020).
[10] *See id.* at 7-9.
[11] TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, REPORT NO. 2020-20-006, ACTIVE DIRECTORY OVERSIGHT NEEDS IMPROVEMENT, at Highlights (Feb. 5, 2020); *id.* at 1–2.
[12] *Id.* at *Highlights*.
[13] *Id.* at 6.
[14] Press Release, IRS Statement on "Get Transcript" (Feb. 26, 2016), https://www.irs.gov/newsroom/irs-statement-on-get-transcript.

compromised through use of a key FAFSA tool.[15] And in 2022, the IRS admitted to mistakenly publishing personal data about 120,000 individuals on its website.[16]

25. A report from the Government Accountability Office in September 2023 also found problems with how the IRS handles taxpayer data.[17] The report found that, since 2010, 77 of the Accountability Office's recommendations for stronger safeguards had gone unheeded. The watchdog agency singled out the 14,000 IRS contractors as a potential weakness, noting that a third of the contractors had not completed a training course on protecting the records of taxpayers. "As a result, IRS contractors [were] at increased risk of being unprepared to handle taxpayer information."[18]

26. The IRS and other related agencies were well-aware of these systemic data security failures. Indeed, the federal government previously retained multiple contractors—Booz Allen among them—to strengthen the IRS's cybersecurity protections.

B. Booz Allen Secures Billions in Government Cybersecurity and Tax Administration Contracts

27. In 2018, the Department of Homeland Security (DHS) issued RFPs for several multiyear contracts to protect the computer networks, electronic data, and IT systems of the IRS and other key government agencies. In February 2018, DHS awarded Booz Allen an initial six-year, $621 million contract to further develop and implement the Department of Homeland

[15] Written Testimony of Kenneth C. Corbin, Commissioner, Wage and Investment Division and Silvana Gina Garza, Chief Information Officer, Internal Revenue Service, Before the House Oversight and Government Reform Committee (May 3, 2017), https://oversighthouse.gov/wp-content/uploads/2017/05/Corbin-Garza-IRS-joint-Statement-FAFSA-5-3.pdf.
[16] *See* Press Release, IRS Statement on Forms 990-T (Sept. 2, 2022), https://www.irs.gov/newsroom/irs-statement-on-forms-990-t; Letter from Anna Canfield Roth, Acting Assistant Secretary for Management, U.S. Department of the Treasury, to Bennie G. Thompson, Chairman of the Committee on Homeland Security (Sept. 2, 2022), https://s.wsjnet/public/resources/documents/IRSBREACH.pdf.
[17] U.S. Government Accountability Office, *Security of Taxpayer Information: IRS Needs to Address Critical Safeguard Weaknesses*, (Aug. 14, 2023), https://www.gao.gov/products/gao-23-105395.
[18] *Id.*

Security's Continuous Diagnostics and Mitigation ("CDM") program, a government-wide cybersecurity effort to monitor and protect federal networks across agencies that included the IRS.

28. In August 2018, Booz Allen secured a second, even more lucrative cybersecurity contract from the same program. DHS, in partnership with the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM), selected Booz Allen as the prime contractor under the government-wide Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) Program for Group D, this time with a larger $1.03 billion task order. At the time, the contract was the largest federal task order and the second-largest cybersecurity task order in Booz Allen's history.

29. The award required Booz Allen to enhance the cybersecurity capabilities of six federal agencies, including the General Services Administration, Department of Health and Human Services, NASA, Social Security Administration, the U.S. Postal Service, and the Department of the Treasury (including the IRS). In securing this contract, Booz Allen claimed to design CDM solutions to help agency leaders understand their attack surface, detect evolving threats, make informed risk-based decisions, and act quickly. Booz Allen also touted its reputation as "the leading provider of professional security services" and its commitment to "bring the best talent and most sophisticated tradecraft together to create innovative cyber solutions at an unprecedented scale."[19]

30. Additionally, in June 2023, Booz Allen announced yet-another IRS award. Booz Allen secured a position on the IRS Enterprise Development Operations Services (EDOS) contract, a blanket purchase agreement that could be worth $2.6 billion over a seven-year period. In this

[19] Press Release, *Department of Homeland Security Awards Booz Allen Hamilton $1.03B Task Order as Prime Contractor to Enhance Cybersecurity Capabilities across Six Federal Agencies*, BOOZ ALLEN (Aug. 21, 2018), https://investors.boozallen.com/news-releases/news-release-details/department-homeland-security-awards-booz-allen-hamilton-103b .

latest contract, Booz Allen will purportedly assist the IRS's IT teams in modernizing systems used to examine and collect taxes by improving efficiencies in tax administration, supporting the IRS's applications development portfolio, and implementing annual tax season legislative requirements.

31. Under these three contracts, as well as several other agreements, the Department of the Treasury and/or IRS contracted with Booz Allen to perform cybersecurity, IT, and tax administration services for the IRS. Under those contracts and agreements, the Treasury Department and the IRS permitted Booz Allen access to IRS databases, computer networks, and other systems containing the tax returns and return information of Plaintiff and other American taxpayers. Booz Allen then provided its employees with access to the IRS's searchable tax return databases and systems, purportedly to perform their work on these government contracts.

32. Under these three contracts alone, Booz Allen has or will receive over $4 billion in federal funds to enhance the cybersecurity of the IRS and other federal agencies. But these taxpayer dollars cannot mitigate the data threats to the IRS. This is because Booz Allen—the very company charged with securing IRS taxpayer data—itself has significant data vulnerabilities that preclude it from securing this sensitive information or performing tax administration services.

C. Booz Allen's Systemic Failures to Secure Confidential Data

33. Booz Allen markets itself as a global leader in cybersecurity technology and consulting, claiming to deliver adversary insight, an innovative approach, and an understanding of advanced threats and vulnerabilities to the most sophisticated global enterprises, government agencies, and national missions.

34. Yet Booz Allen has consistently failed to address its *own* cybersecurity vulnerabilities, and instead has repeatedly permitted its employees to access, download, and disclose highly confidential government and company data. Those failures have been on full display over the last decade.

35. In July 2011, for example, Booz Allen admitted that the hacking group "Anonymous" had infiltrated its company network and stolen a list of approximately 90,000 military email addresses and encrypted passwords. In that breach, Anonymous also misappropriated an assortment of data related to other companies and government networks served by Booz Allen. Anonymous further claimed to have accessed and deleted four gigabytes of the firm's source code and had reportedly discovered "maps and keys" for various government agencies and federal contractors within the Booz Allen unsecured network. Following the breach, Anonymous posted this pithy indictment of Booz Allen's security: "In [Booz Allen's] line of work you'd expect them to sail the seven proxseas [sic] with a state-of-the-art battleship, right? Well you may be as surprised as we were when we found their vessel being a puny wooden barge," explaining that the group had "infiltrated a server on [Booz Allen's] network that basically had no security measures in place."[20] Despite receiving billions in federal contracts related to federal government cybersecurity, Booz Allen's networks apparently lacked the security measures to protect it from a decentralized group of rogue hackers.

36. Unfortunately, Booz Allen chose not to address its data security issues. Instead, it doubled down on its lax policies, repeatedly granting its employees virtually unrestricted access to both internal company servers and the external networks, systems, and databases of its government clients.

37. For example, in early 2013, Booz Allen assigned its employee Edward Snowden, a computer systems administrator, to work on IT systems for the National Security Agency (NSA). By May of 2013, Snowden had used his Booz Allen credentials and access to download thousands

[20] Andy Greenberg, *Anonymous Hackers Breach Booz Allen Hamilton, Dump 90,000 Military Email Addresses,* FORBES (July 11, 2011), https://wwwforbes.com/sites/andygreenberg/2011/07/11/anonymous-hackers-breach-booz-allen-hamilton-dump-90000-military-email-addresses/?sh=7984ac4e76bb.

of top-secret security documents. Snowden fled the United States and leaked the classified materials to multiple journalists, disclosing national secrets and severely compromising the NSA's anti-terror surveillance program. Snowden ultimately fled to Russia, where Vladimir Putin granted him citizenship in 2022.

38. Booz Allen's breaches of government systems continued unchecked. In 2016, authorities arrested Booz Allen computer analyst Harold Martin for stealing approximately 50 terabytes of confidential data from the NSA, in a breach that authorities have called the largest theft of classified information in U.S. history. The 50 terabytes of information from 1996 to 2016 included personal details of government employees and "Top Secret" email chains, handwritten notes describing the NSA's classified computer infrastructure, and descriptions of classified technical operations. Martin's work with Booz Allen involved highly classified projects concerning government computer systems and gave him various security clearances that routinely provided him access to top-secret information. Among the material allegedly stolen by Martin was a top-secret document that contained "specific operational plans against a known enemy of the United States and its allies."[21] Martin ultimately pleaded guilty to a federal charge for stealing classified information.

39. Another significant breach occurred the very next year. In 2017, investigators discovered that Booz Allen had left more than 60,000 confidential or sensitive files on a publicly accessible Amazon Web Services server. Given the files' accessibility, it is highly likely that malicious actors downloaded and used the publicly exposed data. The unguarded data included passwords to sensitive government systems, credentials belonging to a senior engineer at Booz Allen, vulnerability reports on government source code, and identities of government contractors

[21] Government's Response to Defendant's Motion for a Detention Hearing at 4, *United States v. Martin, III,* No. 16-2254-BPG (D. Md. July 19, 2019).

with Top Secret clearances. The exposed files concerned the National Geospatial-Intelligence Agency (NGA), the Department of Defense agency that collects and analyzes data gathered by satellites and drones for the U.S. military and intelligence community. The sensitive data was available for *unrestricted public download* for at least three months in 2017.

40. In November 2022, Booz Allen admitted yet-another significant data breach. Booz Allen's system allowed a single employee to download potentially tens of thousands of other employees' personal information from the company's internal network. Using Booz Allen's network, the employee was able to run a report containing the personal information of "active employees as of March 29, 2021." The report contained the names, Social Security numbers, compensation, gender, race, ethnicity, date of birth, and U.S. Government security clearance eligibility and status for thousands of Booz Allen employees across the company. Booz Allen later admitted the report containing the personal information was "improperly stored on an internal SharePoint site."[22]

41. Even worse, while Booz Allen was failing to secure its own data and that of the government, it was also overcharging American taxpayers under government contracts. In 2023, Booz Allen agreed to pay the United States a massive settlement of $377.4 million to resolve allegations of violating federal law by improperly billing commercial and international costs to its government contracts. The U.S. Government charged that, from 2011–2021, Booz Allen had improperly allocated indirect costs associated with its commercial and international business to its government contracts and subcontracts that either had no relationship to those contracts and subcontracts or were allocated to those contracts and subcontracts in disproportionate amounts.

[22] Booz Allen, *Notice of Event Involving Personally Identifiable Information (PII)* (2022), https://ago.vermont.gov/sites/ago/files/2023-01/2022-11-16-Booz-Allen-Hamilton-Notice-to-Consumer.pdf.

The U.S. Government has called the $377.4 million settlement one of the largest procurement fraud settlements in its history.

D. Booz Allen's Unlawful Access, Use, and Disclosure of Plaintiff's Tax Information

42. These pervasive data security failures and unethical practices culminated in an unprecedented taxpayer data breach by Booz Allen employee Charles "Chaz" Littlejohn.

43. From 2008 to 2010, and then again from 2012 to 2013, Littlejohn worked for Booz Allen, principally under contracts Booz Allen had obtained for IRS work in tax administration, IT services, or cybersecurity work. Booz Allen again hired Littlejohn in 2017 or 2018 as an associate in its finance and economic development practice. Littlejohn remained a Booz Allen employee through approximately 2021, working for Booz Allen on contracts it had obtained from the Department of the Treasury and/or IRS for tax administration, IT services, or cybersecurity work for the IRS.

44. As Littlejohn's employer, Booz Allen maintained direct control over his daily schedule, instructing him on which work to perform, when to perform it, the manner of the work, and for which IRS projects. Booz Allen maintained direct control over the details of Littlejohn's work, including his time spent analyzing IRS data for tax returns and return information, his project assignments, his performance benchmarks, and his performance reviews.

45. Booz Allen issued Littlejohn a computer, as well as network and database credentials, for performing his IRS data projects. Littlejohn was enrolled in the company's regular payroll. Littlejohn's data analysis for the IRS was part of Booz Allen's regular business, for work performed under contracts with the IRS or the Department of the Treasury.

46. On information and belief, Littlejohn took this job to advance his extreme political and ideological agenda. From prior experience on IRS contract work, Littlejohn knew he could freely access unmasked taxpayer data using his unrestricted and unmonitored access from Booz

Allen. And he aimed to use his data clearance to access and disclose tax returns and return information associated with President Trump, as well as other high-net-worth individuals. Littlejohn viewed President Trump as a dangerous threat to democracy, and he intended to obtain the President's taxpayer information from the IRS and provide it to the public. Littlejohn also viewed the U.S. tax system as inequitable, and he believed wealthy Americans had evaded their tax responsibilities and had received disproportionate tax advantages. Littlejohn aimed to weaponize his access to IRS tax data to advance his radical agenda.

47. On information and belief, Booz Allen knew of Littlejohn's extreme political views and his desire to use access to IRS data to promote those views through public disclosure of wealthy Americans' tax information. Yet Booz Allen willingly chose not to monitor Littlejohn's activities or—even worse—knew of those activities, yet blithely ignored them. At all times during Littlejohn's employment, Booz Allen had both the ability and duty to monitor Littlejohn's activities within the IRS database, including his searches, inspections, downloads, transfers, and disclosures of tax returns and return information.

48. Without restriction or supervision from Booz Allen, Littlejohn began using the IRS databases and systems to extract data about President Trump and other high-net-worth individuals, including Plaintiff. Littlejohn used the Booz Allen system and its access to the IRS systems and databases to download confidential tax returns and return information.

49. In late 2018, Littlejohn used his Booz Allen credentials to access the tax returns and return information of President Trump and related entities and individuals.

50. Littlejohn learned that IRS protocols could detect and prevent large downloads or uploads from IRS systems and devices. But on or about November 30, 2018, he exploited a loophole in those controls by using his Booz Allen credentials and computer to upload the stolen

tax returns and return information of President Trump and related entities and individuals to a private website that he controlled. He then used a computer to download the data from that private website. From the original data set stored on his personal computer, Littlejohn made copies and stored them on personal data storage devices such as his Apple iPod (which, using his specialized technical skills, he had configured as a personal hard drive). At all relevant times, Booz Allen allowed Littlejohn to query, inspect, extract, download, transmit, and store this data.

51. Approximately six months later, in or about May 2019, Littlejohn contacted The New York Times to discuss providing it with tax return data on President Trump. Between August and October 2019, Littlejohn disclosed an initial set of President Trump's tax records to The Times. In 2020, Littlejohn stole additional tax returns and return information associated with President Trump. In September 2020, The New York Times published the first of several articles that publicly disclosed the tax information of President Trump.

52. But leaking President Trump's tax returns and return information did not satisfy Littlejohn's agenda of exposing taxpayer data and smearing wealthy Americans.

53. Beginning in July 2020, again without any restriction or monitoring by Booz Allen, Littlejohn repeated his crimes. He began conducting searches to pull historic tax data on the nation's wealthiest taxpayers. Littlejohn constructed a query designed to pull data on hundreds, or even thousands, of wealthy Americans, retrieving data over a fifteen-year period. After running the query, he stole the data set in the same manner as the President's returns, using his Booz Allen computer and credentials to upload the data from the IRS database to his personal website.

54. On information and belief, Booz Allen had no system, supervision, or other controls in place to detect or stop this data breach. Booz Allen did not monitor Littlejohn's activities on IRS systems or databases.

55. In or about September 2020, Littlejohn contacted and discussed with media outlets the possibility of disclosing the tax returns and return information of Plaintiff and thousands of other American citizens.

56. Then, from September 2020 to November 2020, Littlejohn unlawfully disclosed Plaintiff's, and thousands of others' confidential returns and return information using a personal storage device. In or about November 2020, Littlejohn provided journalists with the password to the device. Consequently, numerous articles were published that publicly disclosed data from the returns and return information of Plaintiff Mr. MacNeil and other taxpayers.

57. During much of this time, and in particular between 2018 and 2021, Littlejohn was authorized by Booz Allen to access vast amounts of unmasked taxpayer data, including taxpayer returns and return information, on IRS databases. Indeed, Littlejohn's Factual Basis for Plea confirms he "was authorized, pursuant to 26 U.S.C. § 6103(n), to access vast amounts of unmasked taxpayer data, including taxpayer returns and return information, on IRS databases."[23]

58. Booz Allen willingly allowed Littlejohn to repeatedly inspect—and repeatedly misappropriate—the confidential tax returns and return information of thousands of the nation's wealthiest taxpayers, including Plaintiff. Booz Allen allowed Littlejohn to upload that data to a private website. And Booz Allen allowed Littlejohn to disclose that data to ProPublica.

59. During this time, Mr. MacNeil diligently sought to identify the persons responsible for the unlawful disclosure of his returns and return information to ProPublica. However, the sources of the leak remained hidden. Only on or around the time Littlejohn was indicted on September 29, 2023 did Mr. MacNeil discover the facts necessary to state his claims against Booz Allen. While Booz Allen, ProPublica, or The New York Times were never mentioned by name in

[23] *United States v. Charles Edward Littlejohn*, 1:23-cr-343 (D.D.C.) (ECF 9, ¶ 3, Oct. 12, 2023).

public filings from Littlejohn's criminal proceeding, Plaintiff learned of their identities through investigative reporting, which for the first time, included additional details about (i) Littlejohn's involvement in the leaks, (ii) Booz Allen's involvement in the leaks, and (iii) a more fulsome story of what was leaked and to whom.

60. On information and belief, Littlejohn performed these activities, including extracting and inspecting tax data for high-net-worth individuals, at least in part to benefit Booz Allen because he was requested by Booz Allen to do so, they were tasks Booz Allen expected Littlejohn to perform in the scope of his employment, and/or they reflected his ability and sophistication as an IT employee.

61. The scope and scale of Littlejohn's unlawful disclosures appear to be unparalleled in the IRS's history. There is no precedent for a case involving the disclosure of tax return and return information associated with over a thousand individuals and entities. The human impact of Littlejohn's crimes and Booz Allen's misconduct is enormous. Many victims have come forward, expressing anger and embarrassment about the exposure of their personal financial information.

62. Worse, it appears the harm may continue indefinitely: ProPublica has continued to publish stories using the data disclosed by Littlejohn even after he entered a plea agreement. Plaintiff does not know the full scope of the disclosures made by Littlejohn and has been made aware only of the specific disclosures reflected in the piece-meal stories released by ProPublica. Further, on information and belief, Littlejohn also disclosed Plaintiff's returns and return information to other third party publication sources. Thus, Plaintiff is rightly concerned that additional personal information may be the subject of a news article tomorrow, next week, next month, or even next year. The harm arising from Booz Allen's misconduct and its employee's crimes is extensive and ongoing.

63. The IRS's mission, which is to "[p]rovide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all," cannot be achieved without faith that IRS contractors such as Booz Allen will safeguard citizens' private information. Booz Allen's data breach has undermined that public trust and confidence in the IRS, an institution that is critical to the effective functioning of our government.

64. Moreover, Booz Allen's laxity and misconduct egregiously breaches the trust placed in it by our government. The IRS provided Booz Allen with millions in fees and access to sensitive, unmasked data associated with millions of Americans. Instead of respecting the trust of that agency (and, by extension, hundreds of millions of individuals who shared their information with it), Booz Allen allowed its employee to exploit it for a radical political agenda.

65. Due to the publications of Plaintiff's tax return information, Plaintiff has sustained public backlash, significant reputational harm, loss of privacy, and economic damages from the tax disclosures, along with other harms and damages. Plaintiff brings this suit to seek redress for the unlawful misappropriation and disclosure of his confidential tax information done and allowed by Booz Allen.

VICARIOUS LIABILITY / RESPONDEAT SUPERIOR

66. Plaintiff realleges and incorporates by reference each of the preceding paragraphs as if fully set forth herein.

67. Booz Allen and Littlejohn had an employer-employee relationship.

68. Littlejohn committed tortious acts within the scope of that employment relationship, including unlawfully inspecting and disclosing Plaintiff's tax returns and return information, in violation of 26 U.S.C. § 6103 and Maryland common law.

69. Booz Allen consented—either explicitly or implicitly—to Plaintiff's use of Booz Allen's computers and network access, and access to IRS systems and databases, to perform tortious acts.

70. Booz Allen had the right to control Littlejohn in the operation of his computer, network, and database access, and in his searches, inspections, downloads, and disclosures of confidential tax returns and return information.

71. Littlejohn was motivated to commit these tortious acts at least in part to benefit Booz Allen because he was requested by Booz Allen to do so, they were tasks Booz Allen expected Littlejohn to perform in the scope of his employment, and/or they reflected his ability and sophistication as an IT employee.

72. Accordingly, Booz Allen is vicariously liable for the torts committed by its employee, Littlejohn.

FIRST CAUSE OF ACTION
26 U.S.C. §§ 6103 and 7431

73. Plaintiff realleges and incorporates by reference each of the preceding paragraphs as if fully set forth herein.

74. 26 U.S.C. § 6103 provides that tax "[r]eturns and return information shall be confidential" and applies to any "other person (or officer or employee thereof) who has or had access to returns or return information under . . . subsection (n) . . . ." *Id.* § 6103(a)(3).

75. 26 U.S.C. § 6103(n) permits the disclosure of returns and return information to any person "to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration."

76. "Return" is defined as "any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed." 26 U.S.C. § 6103(b)(1).

77. "Return information" includes "a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense." 26 U.S.C. § 6103(b)(2)(A).

78. Booz Allen is a "person . . . who has or had access to [the] returns or return information" of Plaintiff, under 26 U.S.C. § 6103(n), because the Secretary of the Treasury, pursuant to regulations prescribed by the Secretary, disclosed Plaintiff's returns and return information to Booz Allen "to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration." 26 U.S.C. § 6103(n).

79. Under 26 U.S.C. § 6103(a), no such person who has received tax returns or return information "shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions

of this section." The statute's definition of the term "officer or employee" includes a former officer or employee. *Id.*

80. "[D]isclosure" means "the making known to any person in any manner whatever a return or return information." 26 U.S.C. § 6103(b)(8).

81. 26 U.S.C. § 7431 provides taxpayers a private right of action for damages against any person who is not an officer or employee of the United States for the knowing or negligent unauthorized inspection or disclosure of tax return information in violation of 26 U.S.C. § 6103.

82. On information and belief, Booz Allen, both through its own actions and through its employee, Littlejohn, repeatedly violated 26 U.S.C. § 6103 from 2018 to 2021 by inspecting Plaintiff's confidential tax returns and return information, and then unlawfully disclosing that data to third parties including ProPublica. Those unlawful inspections and disclosures involved confidential information on Plaintiff's income, real property, charitable contributions, financial and securities transactions, adjusted gross income, and information sufficient to calculate the purported effective federal income tax rates he paid over at least a decade.

83. Booz Allen made these unlawful inspections and disclosures knowingly, or at the very least negligently or with gross negligence, including because the inspections and disclosures were made while willfully failing to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's confidential taxpayer information from the unlawful inspections and disclosures alleged herein.

84. Booz Allen made these unlawful inspections and disclosures knowingly, or at the very least negligently or with gross negligence, including because the inspections and disclosures were made while willfully failing to adequately supervise the activities of employees, such as

Littlejohn, that it knew to be incompetent and capable of inflicting harm through an unauthorized inspection or disclosure of tax returns or return information.

85. Booz Allen, both through its own actions and through its employee, Littlejohn, unlawfully inspected and disclosed Plaintiff's tax returns and return information using Booz Allen's computers and network access to IRS systems and databases. The unlawful inspections and disclosures were made within the scope of Littlejohn's employment at Booz Allen.

86. Booz Allen, both through its own actions and through its employee, Littlejohn, caused the disclosure of the confidential return information to third parties including ProPublica with the intent that news organizations would widely publish the information through their websites or through other means.

87. Booz Allen's inspections and disclosures of Plaintiff's tax return information did not result from a "good faith, but erroneous interpretation of section 6103," *see* 26 U.S.C. § 7431(b)(1), but rather from knowing violations, gross negligence, and/or negligence.

88. Booz Allen's inspections and disclosures of Plaintiff's tax return information were not "requested by the taxpayer," Plaintiff, pursuant to 26 U.S.C. § 7431(b)(2).

89. Pursuant to 26 U.S.C. § 7431(c), Plaintiff is entitled to statutory damages in the amount of $1,000 for each act of unauthorized inspection and disclosure, plus actual damages sustained as a result of the unauthorized inspections and disclosures.

90. Plaintiff is also entitled to punitive damages pursuant to 26 U.S.C. § 7431(c)(1)(B)(ii) because Booz Allen's unlawful inspections and disclosures of his confidential tax return information were either willful or a result of gross negligence.

91. Plaintiff is entitled to the costs of the action and reasonable attorney's fees pursuant to 26 U.S.C. § 7431(c)(3) if he is the prevailing party in this action.

SECOND CAUSE OF ACTION
Invasion of Privacy (Maryland Common Law)

92. Plaintiff realleges and incorporates by reference each of the preceding paragraphs as if fully set forth herein.

93. At all relevant times, Booz Allen had access to the private tax returns and return information of Plaintiff.

94. Plaintiff's taxpayer returns and return information are, and are entitled to be, private facts.

95. Plaintiff's tax returns and return information are matters the disclosure of which are highly offensive to a reasonable person and are matters that are not of legitimate concern to the public.

96. Unbeknownst to Plaintiff, in or about September 2020, Booz Allen, acting through Littlejohn, contacted and discussed with ProPublica the possibility of unlawfully disclosing a copy of Plaintiff's and thousands of others' confidential tax return information.

97. Booz Allen, acting through Littlejohn, disclosed the taxpayer data—including that of Plaintiff—via an encrypted USB drive to a ProPublica journalist. Then, Booz Allen unlawfully disclosed Plaintiff's and thousands of others' confidential returns and return information to ProPublica on a personal storage device.

98. Later, Booz Allen, acting through Littlejohn, disclosed the device's password to ProPublica. ProPublica then published nearly 50 articles that publicly disclosed data from the returns and return information of Plaintiff and other taxpayers.

99. At all relevant times, Littlejohn was acting, at least in part, with an intent to benefit Booz Allen.

100. Booz Allen, acting through its employee, thus made the private facts of these returns and return information public by disclosing them to journalists, who then published them on the internet. The inspection and disclosure of the tax returns and return information were done with actual malice, evil motive, and intent to injure. Specifically, Booz Allen's employee Littlejohn inspected and disclosed Plaintiff's tax returns with the intention to cause, *inter alia*, public backlash, significant reputational harm, loss of privacy, and economic damages to Plaintiff.

101. Booz Allen's public disclosure of Plaintiff's tax returns and return information gave publicity to a matter concerning the private life of Plaintiff.

102. Booz Allen's public disclosure of Plaintiff's tax returns and return information proximately caused Plaintiff's injuries.

JURY DEMAND

103. Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff demands a trial by jury of all claims asserted in this Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court enter judgment in his favor and against Booz Allen, as follows:

i. Declaring that Booz Allen willfully, knowingly, and/or by gross negligence, unlawfully inspected Plaintiff's confidential tax return information in violation of 26 U.S.C. § 6103;

ii. Declaring that Booz Allen willfully, knowingly, and/or by gross negligence, unlawfully disclosed Plaintiff's confidential tax return information in violation of 26 U.S.C. § 6103;

iii. Awarding Plaintiff $1,000 in damages for each unauthorized disclosure of his tax return information, or actual damages sustained by Plaintiff as a result of the unauthorized inspection or disclosure, pursuant to 26 U.S.C. § 7431(c)(1);

iv. Awarding Plaintiff reasonable costs and attorney's fees pursuant to 26 U.S.C. § 7431(c)(2)-(3) and as may otherwise be permitted by law;

v. Awarding Plaintiff punitive damages pursuant to 26 U.S.C. § 7431(c)(1)(B)(ii) because Booz Allen's unlawful disclosure of his confidential tax return information was either willful or a result of gross negligence;

vi. Awarding Plaintiff actual damages, punitive damages, and costs of suit under Maryland common law;

vii. Awarding pre-and post-judgment interest as allowed by law; and

viii. Any such other relief the Court deems just and proper

Dated: March 24, 2025

Respectfully submitted,

/s/

Dwight W. Stone II, Bar Number 22968
Ariana K. DeJan-Lenoir, Bar Number 20522
MILES & STOCKBRIDGE P.C.
100 Light Street
Baltimore, MD 21202
dstone@milesstockbridge.com
adejanlenoir@milesstockbridge.com
(410) 385-3649

ATTORNEYS FOR PLAINTIFF DAVID MACNEIL